**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software
   1. What are the two types of modern encryption methods?

* Symmetric-key encryption: both the sender and the receiver have the same shared key installed on their computers. The sender uses the key to encrypt a packet of information before sending it over a network to the recipient.
* Asymmetric-key encryption: uses two keys, a public and a private key. Your public key is given by your computer to any computer that wants to communicate securely with it. The private key remains known only to your computer.

1. Network policies, profiles

* Many organisations now use networks to enable employees to access data stored in different locations. In some cases staff members may be located in different parts of the world, but working together on a single document.

1. Firewalls

* Firewalls are another type of network protection, used to restrict access by outsiders to a network, as well as to protect confidential information such as payrolls and personnel records from employees not authorised to access it.

1. Antivirus software

* Can be used to prevent computer virus infections. This software detects the presence of viruses as the computer boots up, when an executable file is run, when documents are accessed or when files are copied.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

* Well-documented processes for communicating sensitive information via email, telephone and fax
* Use of passwords on documents that have sensitive information
* Well-documented policy for the use of networked devices within the organisation

**Storage**

1. **File-naming conventions**
   1. List the 3 types of information each document should include.

* Date stamp
* Variation
* Name

1. **Location of files**

* When storing files on a network server an organisation may set a directory structure to control where employees store their files so that documents can be easily located

1. **Backups**
   1. Distinguish between each of the following:
      1. Full backup
      * Copied all files from a device to a storage medium
      1. Differential backup
      * Copied only those files that have been changed since the last full backup
      1. Incremental backup
      * Similar to a differential backup, the difference being that it uses more than two backup media, while a differential backup uses only two media
2. **Backup timeline**
   1. List good practice in relation to backup timelines.

* As soon as a file is changed
* Larger organisations back up constantly as there are usually financial ramifications for the loss of data

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

* Your backups should be stored in a location that is safe from theft and damage caused by extremes of temperature or disasters.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

* Archiving is essentially a process of copying files to long term storage, then deleting them from the hard disk. Destruction involves deletion only.
  1. What is a problem for ICT managers?
* The problem for ICT managers is determining which is the most appropriate long term storage medium to use.
  1. What is a legacy system?
* A legacy system is an old system that might run old databases on old servers or mainframes.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

* Protecting sensitive and private data as no techniques can completely guarantee that the information is completely disposed of.